Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) A device, comprising:

at least one interface configured to receive data transmitted via a network;

a firewall configured to:

receive data from the at least one interface,

determine whether the data potentially contains malicious content, and

identify first data in the received data that potentially contains malicious content;

intrusion detection logic configured to:

receive the first data, and

generate report information based on the first data; and

forwarding logic configured to:

receive the report information, ~~and~~

~~determine whether to forward the first data for processing by a user application based on the report information~~

forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and

forward the report information to a remote central management system when the report information indicates that the first data potentially contains malicious

content, the report information allowing the remote central management system to make a forwarding decision on behalf of the device.

2. (canceled)

3. (canceled)

4. (currently amended) The device of claim [[3]]1, further comprising:

a virtual private network gateway configured to establish a secure connection with the remote central management system.

5. (currently amended) The device of claim 1, wherein the firewall comprises anti-virus logic configured to examine a data stream for viral signatures using at least one of a signature-based technique, a heuristic technique [[and]]or a rough set logic technique.

6. (original) The device of claim 5, wherein the anti-virus logic is further configured to identify unsolicited messages.

7. (currently amended) The device of claim 1, further comprising:

a processing device executing the user application, the user application being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files [[and]]or downloading games.

8. (currently amended) The device of claim 1, wherein at least one of the firewall, the intrusion detection logic [[and]]or the forwarding logic is configured to receive rule-based processing information from an external device via the network.

9. (currently amended) The device of claim 8, wherein at least one of the firewall, intrusion detection logic [[and]]or forward logic is further configured to receive updated rule-based processing information from the external device.

10. (currently amended) In a network device configured to receive data transmitted over a network, a method, comprising:

receiving data transmitted via the network;

identifying first data that may contain malicious content;

generating report information based on the first data;

~~determining, based on the report information, whether to forward the first data for processing by a user device;~~

forwarding the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the network device; and

forwarding the first data to the user device when it is determined that the first data does not contain malicious content.

11. (canceled)

12. (currently amended) The method of claim [[11]]10, further comprising:

establishing a virtual private network connection to the external device, and wherein the forwarding the report information includes:

forwarding the report information over the virtual private network connection.

13. (currently amended) The method of claim [[11]]10, further comprising:

receiving, from the external device, information indicating whether the first data is to be forwarded to the user device; and

dropping the first data when the information indicates that the first data is not to be forwarded.

14. (currently amended) The method of claim 10, wherein the identifying comprises:

examining the received data for viruses using at least one of a signature-based technique, a heuristic technique [[and]]or a rough set logic-based technique.

15. (original) The method of claim 10, wherein the identifying comprises:

identifying spam.

16. (currently amended) A computer-readable medium having stored thereon a plurality of sequences of instructions, said sequences of instructions including instructions which, when executed by a processor, cause the processor to:

receive data transmitted via a network;

receive at least one set of rules from an external device, the at least one set of rules being associated with processing the received data;

determine whether the data may contain malicious content using a first set of rules;

identify first data that may contain malicious content based on the determining; ~~and~~

~~determine whether to forward the first data to a user device based on a second set of rules.~~

generate report information based on the first data;

forward the first data for processing by a user application when the report information indicates that the first data does not contain malicious content; and

forward the report information to an external device when the report information indicates that the first data potentially contains malicious content, the report information allowing the external device to make a forwarding decision on behalf of the processor.

17. (canceled)

18. (canceled)

19. (currently amended) The computer-readable medium of claim [[18]]16, wherein the instructions further cause the processor to:

establish a virtual private network tunnel with the external device and send the report information over the virtual private network tunnel.

20. (currently amended) The computer-readable medium of claim 16, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify a virus using at least one of a signature-based technique, a heuristic technique [[and]]or a rough set logic-based technique.

21. (original) The computer-readable medium of claim 20, wherein when identifying first data that may contain malicious content, the instructions cause the processor to identify spam.

22. (currently amended) The computer-readable medium of claim 16, wherein the instructions further cause the processor to execute the received data, the data being associated with at least one of video-on-demand, video-based training, on-line gaming, on-line shopping, downloading music files [[and]]or downloading games.

23 – 28. (canceled)